UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF VIRGINIA
CHARLOTTESVILLE DIVISION

UNITED STATES OF AMERICA

v.

HAIZHOU HU

Case No. 3:20mj00036

AFFIDAVIT IN SUPPORT OF A CRIMINAL COMPLAINT

I, Matthew S. Rader, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent with the Federal Bureau of Investigation (FBI) and have been since November 2005. I am currently assigned to the Richmond Division of the FBI, Charlottesville Resident Agency. I received formal training at the FBI Academy in Quantico, Virginia, on, among other things, the United States Constitution, federal criminal statutes and rules, and conducting criminal and national security investigations, to include writing and executing search and arrest warrants. My principal duties include the investigation of various criminal violations, to include espionage, economic espionage, theft of intellectual property and trade secrets, and

unauthorized access of computer systems. In the course of my career with the FBI, I have been involved in the execution of numerous federal arrest warrants.

2. I make this affidavit in support of a criminal complaint charging HU HAIZHOU (HAIZHOU HU), with fraud and related activity in connection with computers in violation of 18 U.S.C. § 1030, and theft of trade secrets in violation of 18 U.S.C. § 1832.

3. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is sufficient probable cause to charge HU for the offenses listed above and does not set forth all of my knowledge about this matter.

RELEVANT STATUTES

4. Title 18, United States Code, Section 1030(a)(2) provides: "Whoever . . . intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer" commits a federal criminal offense.

5. Title 18, United States Code, Section 1832 provides: Whoever, with intent to convert a trade secret, that is related to a product or service used in or intended for use in interstate or foreign commerce, to the economic benefit of anyone other than the owner thereof, and intending or knowing that the offense will, injure any owner of that trade secret, knowingly— (1) steals, or without authorization appropriates, takes,

carries away, or conceals, or by fraud, artifice, or deception obtains such information; (2) without authorization copies, duplicates, sketches, draws, photographs, downloads, uploads, alters, destroys, photocopies, replicates, transmits, delivers, sends, mails, communicates, or conveys such information; (3) receives, buys, or possesses such information, knowing the same to have been stolen or appropriated, obtained, or converted without authorization; or attempts or conspires to do so commits a federal criminal offense.

BACKGROUND

6. On August 25, 2020, U.S. Customs and Border Protection (CBP) agents assigned to Chicago's O'Hare International Airport were conducting routine screening of outbound travelers in the boarding process for China Eastern flight #MU 7226 to Qingdao, China. One of those travelers was an individual by the name of HAIZHOU HU. When CBP questioned HU regarding the nature of his activities in the United States, HU – as noted below – provided conflicting and incriminating statements regarding his activities while conducting U.S.-government funded research at the University of Virginia (UVA) Department of Mechanical and Aerospace Engineering (MAE) under the guidance of an individual, referred to in this affidavit as Professor 1. A review by CBP of portions of HU's electronic devices revealed UVA-research related

files stored on HU's laptop, to include bio-inspired research[1] simulation software code developed by Professor 1. HU did not have lawful, authorized access to this material, and he admitted that Professor 1 would not want him to have it and would be upset to learn that HU possessed it. Professor 1 has been developing this code over the last 17 years.

PROBABLE CAUSE

7. During the interview with CBP, HU said he was conducting research at UVA on bio-mimics and fluid dynamics to be used in underwater robotics, submersible vehicles, aircraft engines, and various other marine and aerospace applications. HU knew that this research was funded by the United States government in the form of a grant by the U.S. National Science Foundation (NSF), which is an independent federal agency created by Congress to promote the progress of science, advance the national health, and secure the national defense. HU stated Professor 1 runs the Flow Simulation Research Group (FSRG) that is a multi-university collaborative funded by the Office of Naval Research. HU approached Professor 1 to ask about conducting research at UVA after Professor 1 had given a lecture on bio-mimics in aerodynamics at Beihang University in 2017. HU stated the costs associated

[11] "Bio-inspired" research refers to the development of processes, materials, or devices by using biological structures or processes as inspiration. For example, studying the wings of a bird in order to develop an airplane, or the fins of a fish in developing a submersible vehicle.

with his research in the United States were paid for by a scholarship from the Chinese Scholarship Council (CSC).

8. HU said that he works for the Chinese Key Laboratory for Fluid Dynamics located at Beihang University. HU stated that the Chinese-equivalent of the NSF funds the Key Laboratory, and that the Key Laboratory also receives funding from the Chinese Air Force. According to the Curriculum Vitae submitted with his U.S. visa application, HU had previously attended a Chinese University named "Harbin University." Hu told CBP agents that, at Harbin University, he worked in the Key Laboratory for Underwater Robot Technology. When asked how that laboratory was funded, at first, HU said he was not sure. HU was then asked if the laboratory was funded by the People's Liberation Army ("PLA"), which is the armed forces of the People's Republic of China, to which HU replied: "Of course." HU stated that, as part of his scholarship, he was directed by the Chinese Scholarship Council to upload summary reports regarding his UVA research every 6 months.

9. HU was asked if his electronic devices stored any of the research that he conducted at UVA. HU stated he had all of his research on his devices. At first, HU indicated that Professor 1 knew he was taking his research with him. Later, HU stated that neither Professor 1 nor anyone else was aware he was taking his research with him back to China.

10. A basic media exam of the HU's Lenovo laptop, 2 external hard drives, 1 flash drive, iPad, and 2 cell phones was conducted and HU's devices were detained.

During the interview, HU admitted he had coding files on his computer that Professor 1 would not want him to have and would be upset to learn that HU possessed it. Subsequent review of HU's laptop identified approximately 9,600 F90 FORTRAN source code files used for bio-inspired learning, research, and modeling.

11. On August 26 and 27, 2020, agents of the Federal Bureau of Investigation and Customs and Border Patrol interviewed Professor 1, who is a Professor at the University of Virginia's Department of Mechanical and Aerospace Engineering. Professor 1 knew HU and confirmed that HU had been a researcher in Professor 1's laboratory from approximately March 2019 to August 2020. Professor 1, who was HU's research sponsor, stated that HU had left UVA to return to China without contacting him to bid him farewell, which he found unusual.

12. Professor 1 stated the F90 source code files were used during simulations conducted in furtherance of his bio-inspired fluid mechanics research funded by NSF. Professor 1 categorized the file types utilized in his research simulations into four categories: 1) Pre-processing code; 2) Executable files; 3) Post-processing data; and 4) the "core code." According to Professor 1, researchers – including HU – who were conducting simulations in Professor 1's laboratory at UVA had access to the first three types (i.e., pre-processing code, executable files and post-processing data). However, as to the "core code," the access was strictly guarded. According to Professor 1, these strict limitations were by design because the core code was proprietary and he had been developing the code over the last 17 years. Professor 1 further described the core

code as the preeminent bio-inspired research simulation software in the world. Other universities and commercial vendors have requested access to the core code for both research and commercial uses, which includes use in underwater robotics, submersible vehicles, aircraft engines, and other marine and aerospace applications. However, Professor 1 has not shared it because he wishes to maintain his – and the University of Virginia's – unique competitive advantage in conducting research in the bio-inspired fluid mechanics field.

13. Because of the importance and value of the core code, only three people have access: Professor 1 and two graduate students who work under Professor 1 on his continued development of the core code (Authorized Students 1 and 2). Professor 1's ability to conduct simulations using this core code resulted in his receiving numerous grants as a researcher, including but not limited to 2 current NSF grants totaling $1.8 million dollars. According to a UVA Applied Research Institute official, a U.S.-based company, Company One, has developed similar simulation software for use in engineering simulation and modeling, and vendors pay Company One a yearly fee to be able to use such software; open source reporting indicates Company One's revenue in 2019 exceeded $1.5 billion dollars.

14. The core code is stored on a UVA high performance computer cluster (referred to here as Cluster A) in UVA's data center to which physical and electronic access is strictly controlled. Cluster A is located on the grounds of the University of Virginia in Charlottesville, Virginia, within the Western District of Virginia, and only

University of Virginia IT personnel may physically access the building and room where Cluster A resides.

15. Some researchers in Professor 1's laboratory may access Cluster A through UVA's Virtual Private Network (VPN). UVA's VPN advises all individuals using the network:

> You are now connected to the University of Virginia network, which is available for authorized use only. All traffic and actions are subject to University's policies (http://uvapolicy.virginia.edu/). By connecting to the university's network, you acknowledge and consent to these terms.

16. UVA's policy entitled, "IRM-002: Acceptable Use of the University's Information Technology Resources," states, among other things, that users must not:

- Obtain or attempt to obtain unauthorized access to the University's IT resources; [and]
- Circumvent or attempt to circumvent security controls on the University's IT resources [.]

17. For every researcher who has access to Cluster A, their access is individually reviewed and approved by Professor 1 and then administered by UVA's Information Technology personnel. Each researcher's profile determines what information on Cluster A they are able to access. Each individual researcher has a "home" storage space that only that individual can access, and each individual may also access a "shared" storage space which is shared among other users. Professor 1 stored his core code on the home storage space for himself and Authorized Students 1 and 2, the two graduate students with whom he works closely on the core code. By

design, and in order to safeguard the core code, no other researchers had access to his code in their home drive or shared storage space on Cluster A, including HU. Access to each researcher's profile on Cluster A is controlled by entering unique username and password.

18. Over the course of his research in the laboratory between March 2019 and August 2020, HU asked Professor 1 for access to Professor 1's core code on multiple occasions. Each time, Professor 1 denied his request. HU asked Professor 1 for access to Cluster A, the high-performance computer cluster on which the code resides, but only in the home storage of the three aforementioned individuals. Professor 1 granted HU access to Cluster A's shared storage space, but prior to granting HU access, Professor 1 reviewed the contents of the shared storage space to ensure no core code files were present. Professor 1 stated HU requested access to the core code from both of the UVA graduate students within his lab with access, but both denied HU's request.

19. On August 27, 2020, Professor 1 and FBI agents reviewed the code files that were located on HU's laptop computer he sought to take outside of the United States to China. Using a keyword search, Professor 1 and agents identified approximately 55 of his core code files. Professor 1 indicated the files constituted the entirety of his core code he had been developing over the last 17 years and he did not know how HU obtained the files. Professor 1 told the FBI that there were only a few ways that HU could have obtained this material: (1) by using credentials stolen from

Professor 1 or Authorized Students 1 or 2; (2) by accessing the core code when an person with authorized access was logged in but walked away from their computer, or (3) using other methods, such as a password cracking tool, and the like, to hack into the storage space where the core code was stored. Professor 1 was extremely concerned with the prospect of his core code being taken for use outside his research lab, as it would compromise his competitive advantage in his research field and could be exploited for various commercial, governmental and military applications by other entities, including universities, companies, or countries.

20. On August 28, 2020, FBI agents contacted Authorized Students 1 and 2. Both individuals told the FBI that they did not provide HU with the core code, nor did they give HU access to their profile on Cluster A.

CONCLUSION

21. Based on the foregoing, I submit there is probable cause to charge HAIZHOU HU for the offenses fraud and related activity in connection with computers in violation of 18 U.S.C. § 1030(a)(2), and theft of trade secrets in violation of 18 U.S.C. § 1832.

OATH

The information in this affidavit is true to the best of my knowledge and belief.

Respectfully submitted,

s/Matthew S. Rader
Matthew S. Rader, Special Agent
Federal Bureau of Investigation

Received by reliable electronic means and sworn and attested to by telephone on this 28th day of August 2020.

JOEL C. HOPPE
UNITED STATES MAGISTRATE JUDGE